CHAPTER 6
CONTROL SYSTEMS

6-1. Controls system design criteria

C4ISR facility systems require the highest possible level of reliability. This is also true of the SCADA systems used to monitor and control the mechanical and electrical systems. In general, the control system layout should mirror the design of the utility systems: if there is an N+2 equipment layout, there should be at least an N+2 control hardware architecture (see paragraph 2-7, Reliability Criteria). All systems should meet the following basic design criteria:

a. The expected lifetime of the hardware and software for the control system should be greater than 15 years.

b. The control system architecture should be designed to achieve maximum reliability.

c. No single failure should be able to disable the command center or multiple peripheral zones.

d. An N+2 design should be implemented to meet the RAM design criteria. In this design, one area can be out of service for known reasons (such as maintenance) and another area can be out of service for unplanned reasons (such as equipment failure or a terrorist event).

e. The costs of cable installation should be taken into account. In other words, communication cables should be used instead of long-distance runs of multiple conductors whenever possible.

f. Peripheral zone systems and equipment should be controllable remotely from the command center and locally at the zone.

g. The control system hardware should be more reliable than the equipment being controlled, such as pumps and motors (high mean time to fail [MTTF]).

h. A single control system failure should affect only one piece of equipment for a limited time duration (low mean time to repair [MTTR]).

i. The use of proprietary hardware, software, and communications should be avoided.

j. Control equipment should be scaled properly, that is, using small systems for small input/output (I/O) counts and large systems for large I/O counts.

6-2. Applicable control systems codes and standards

The following specific standards apply to the design of control systems to support the LVD concept:

a. ANSI/[Instrumentation, Systems, and Automation Society] ISA 84.01, Application of Safety Instrumented Systems for the Process Industries.

b. TM 5-601, Supervisory Control and Data Acquisition Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities

6-3. Agent detection

The detection of CBR agents is a fast-developing area of technology. Many government agencies are working on these technologies. Two of the best sources of the latest information are the Technical Support Working Group (TSWG) and the Centers for Disease Control and Prevention (CDC). Their respective websites are www.tswg.gov and www.cdc.gov. No single device or instrument is expected to be capable of detecting all three types of agents. At least three independent agent detection systems are expected to be required as inputs to the facility SCADA system. A promising area of research involves the use of nanotechnology to develop instruments to detect not only the release of a CBR agent but also the specific agent. This is part of a technology group called Micro-Electrical/Mechanical Systems (MEMS) and Micro-Optical Electrical/Mechanical Systems (MOEMS).

a. Some of the most common forms of instrumentation to detect chemical agents are as follows (according to Griffin Davis, MD, MPH, and Gabor Kelen, MD, *[Chemical, Biological, Radiological, Nuclear and Explosives] CBRNE – Chemical Detection Equipment*):

(1) Ion Mobility Spectrometer (IMS) – Ion mobility detection is based on the transit speed of chemical agents. This technology is available in handheld devices, fixed site detectors, and remote agent detectors. IMS is the basis of most chemical agent detectors made today. It can detect agents such as nerve gas, mustard gas, and vesicants (chemicals that cause skin blisters). The military already uses a standalone detector called the M8A1, made by Environmental Technologies Group (ETG). A commercial version of this device is also available that can transmit information remotely, as is required for a C4ISR facility that incorporates the LVD concept.

(2) Infrared Spectrometer (IRS) – Infrared technology looks at the different wavelengths detected in the chemical agent and compares them to the known spectral analysis of each agent. The military uses an M21 Remote Sensing Chemical Agent Alarm (RSCAAL) in the field.

(3) Miniature Automatic Continuous Agent Monitoring System (MINICAMS) – This technology uses gas chromatography with flame photometry and enables more specific detection but takes about 3 to 5 minutes to complete each detection cycle.

(4) Surface Acoustic Wave (SAW) – This technology uses chemically selective coated crystals that change frequency when detecting a chemical agent. This change can be detected by a microcomputer, thus making the device relatively inexpensive. It is commonly used by civilian response units.

b. Some of the most common forms of instrumentation to detect biological agents are as follows (according to [National Institute of Justice] NIJ Guide 101–00):

(1) Wet detection (flow cytometry) instruments – This technology measures cells and particles in a moving fluid as they pass through a testing point. The biological agent can be identified by using laser light scattering, electronics, and computers. Such instruments are made by the Los Alamos National Laboratory and the Becton Dickenson Company.

(2) Bacterial spore detection instruments – This technology is made by the Universal Detection Technology Company and acts as an "anthrax smoke detector." It detects the chemical dipicolinic acid, which is inside any bacterial spore. It is suitable for continuous sampling, with detection occurring within 15 minutes of the attack.

(3) Dry detection (mass spectrometry) instruments – This technology uses mass spectrometry to obtain characteristic information on the structure and molecular weight of the sample. The following are the dry detection instruments of this type:

(a) Chemical Biological Mass Spectrometer (CBMS)

(b) Pyrolysis-Gas Chromatography-Ion Mobility Spectrometer (PY-GC-IMS)

(c) Matrix-Assisted Laser Desorption Ionization-Time of Flight-Mass Spectrometry (MALDI-TOF-MS)

c. For radiological agent detection, both military and commercial detectors are available. Another consideration is the presence of "dirty bombs," which have a different radiological signature than most sources. There are some companies that make detectors for this type of attack.

6-4. Distributed architecture

TM 5-601 discusses a variety of possible control system architectures. All C4ISR facilities should have a distributed architecture, which inherently protects against internal control system failures and their consequences. The protection of individual control components from any external threat is not economically feasible. Therefore, the principal means of protection is the control cabinet itself and its environmental protection rating.

6-5. Reliability

Figure 6-1 shows a control equipment plan for the example C4ISR facility to which the LVD principles have been applied.

a. Zones 1 through 4 each contain not only the zone's mechanical and electrical equipment but also the associated control equipment. Each zone contains a control panel for the mechanical equipment and a panel for the electrical equipment. Typically, these panels are supplied with the equipment. In the example facility, the programmable logic control (PLC) in the electrical panel is replaced by a remote I/O communications module communicating to the PLC in the mechanical panel. Both the mechanical and electrical "programs" reside in the same PLC processor. In addition, the mechanical panel has an operator interface terminal (OIT), housed in the front of the panel, as the means by which an operator can control and monitor the equipment in that zone. With the facility intercommunication system, an operator can also monitor Zones 1 through 4 but not Zone 5, the command center.

b. All peripheral zone PLCs are connected to Ethernet switches by fiber optic communications cables. The Ethernet switches are all housed within Zone 5 and connected in a "self-healing" ring topology, as shown in figure 6-2. The fiber optic cables should be the loose-tube type to avoid damage by shock. In addition, Zone 5 contains the following:

(1) A redundant PLC system

(2) A redundant remote I/O system

(3) Six interconnected Ethernet switches

(4) A human-machine interface (HMI) system for monitoring and controlling all zones in the facility

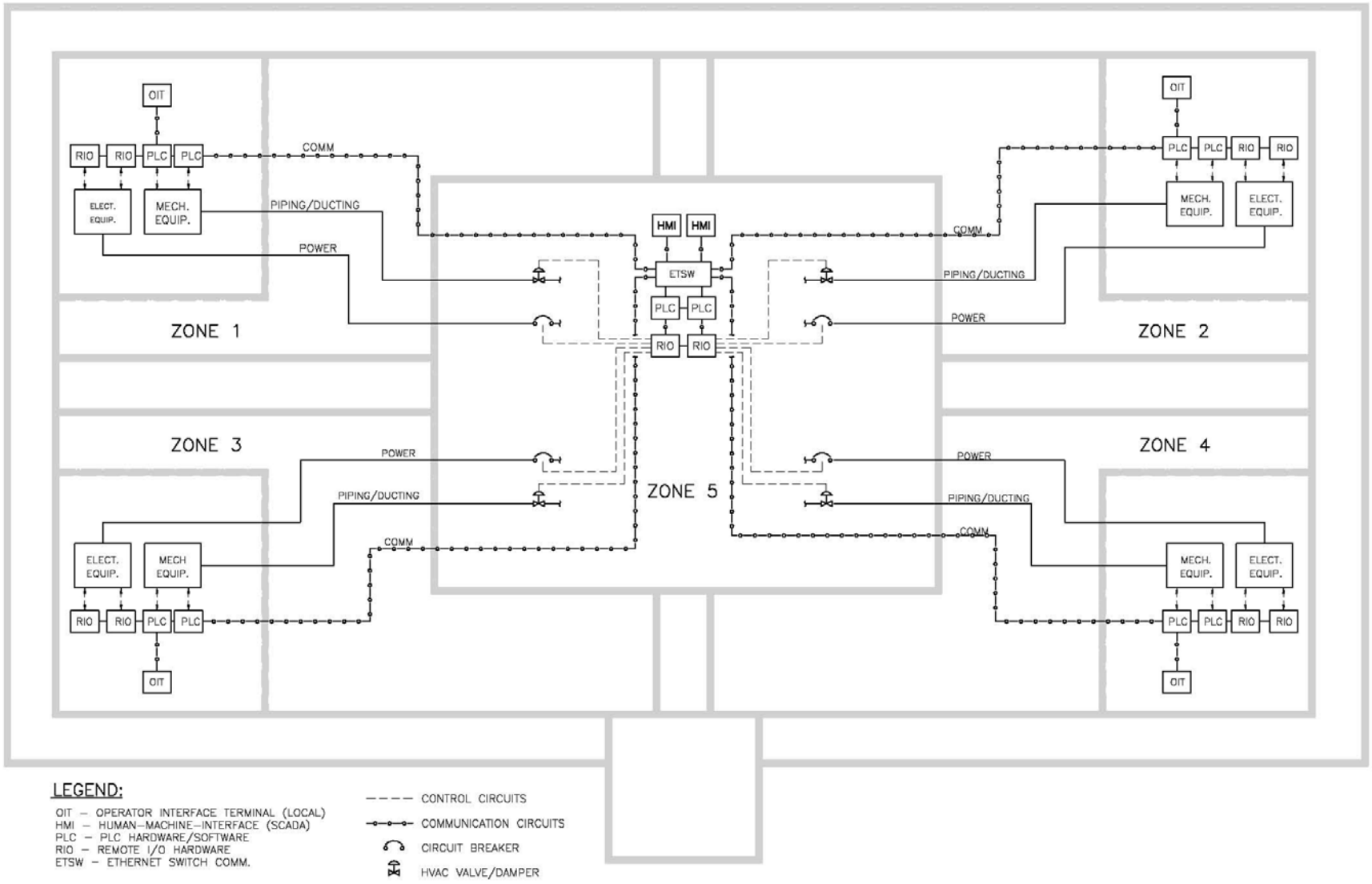

Figure 6-1. SCADA system architecture for the example facility

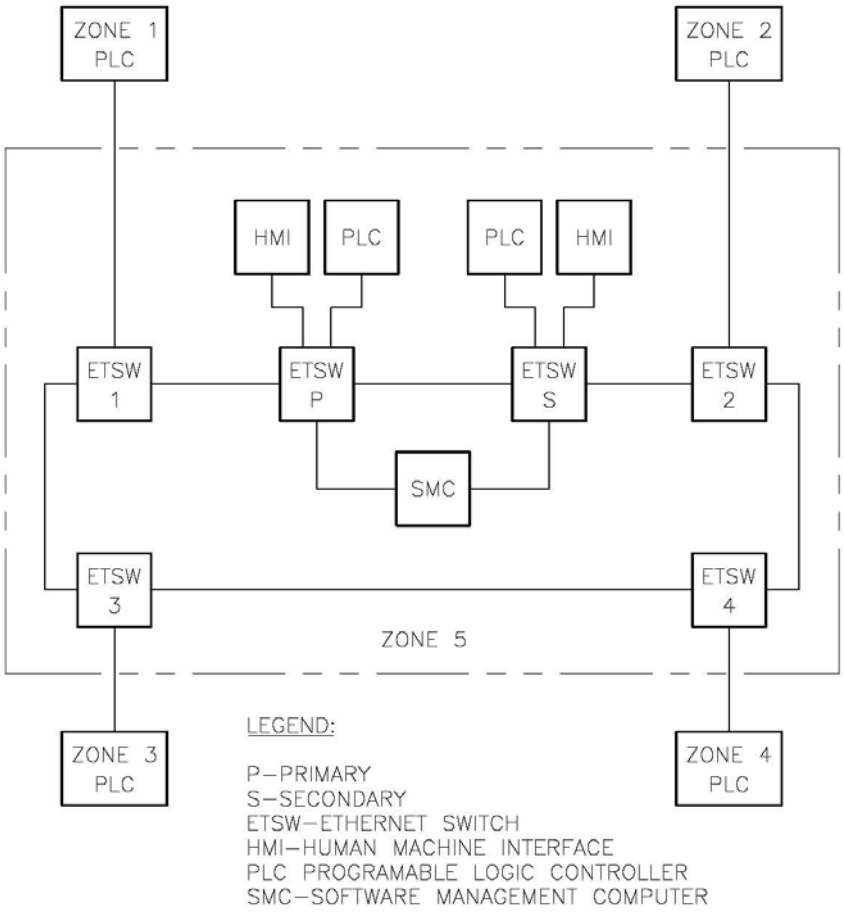

Figure 6-2. Ethernet switches in self-healing ring topology

(5) Each zone's mechanical and electrical isolation equipment (which is controlled by the Zone 5 PLC)

(6) A security computer connected to the communications network

c. The security computer contains specialized, commercially available software that monitors the health of all devices on the network. It also controls access to each PLC, HMI, or OIT to ensure the complete integrity of the control system and not allow unauthorized access to the application or system software. For more information on the security computer and its software, see TM 5-601.

d. There are two possible ways to implement the required redundancy in Zone 5. Figure 6-1 shows the use of PLC equipment with redundant processors and I/O hardware. In this configuration, I/O signals are wired to two different remote I/O racks, which communicate to two PLC processors in separate chassis with their own power supplies and backup communication modules. In this configuration, one PLC is the primary and the other PLC is designated the secondary. These PLCs use the backup communication modules to determine what the status of the PLCs is and which PLC controls the I/O subsystem and communications.

(1) Another option is to use commercially available PLC equipment in which the redundancy is built into the PLC hardware through the use of "two out of three" voting logic. This configuration is a single-chassis PLC system that has redundant power supplies and two or three processors.

(2) The processors communicate to each other through the chassis backplane and execute "two out of three" voting logic to all input and output modules. The system is programmed as if there were only one processor.

6-6. Survivability

With the control equipment plan described in paragraph 6-5, Reliability, the way in which this system would operate can be analyzed.

a. Each zone would have its own detection equipment for CBR agents. The expectation is that the detection equipment would be small devices much like smoke detectors. The interface to the local PLC could range from a simple switch to an analog measurement to a serial communication interface, depending on the sophistication of the device.

(1) The latter interface would not only detect the agent but would identify the agent as well. Once the agent is identified predetermined protocols would take place to minimize the damage. This would be the ultimate goal of any technology involved with agent detection.

(2) As an example, if the Zone 1 PLC detected a CBR event, the OIT of Zones 2, 3, and 4 would show that alarm via each zone's respective PLC. The Zone 5 PLC would react to the alarm by isolating the Zone 1 mechanical and electrical equipment via the valves and breakers located within Zone 5. All other isolation valves and breakers would remain in their normal position so that Zone 5 receives services from Zones 2, 3, and 4. Each unaffected zone system would implement the HVAC pressurization strategy described in paragraph 4-6, Heating, Ventilation, and Air-Conditioning Systems.

b. A very important feature of this design is that Zone 1 does <u>not</u> control the mechanical and electrical isolation equipment between Zone 1 and Zone 5. This logic also follows for the other zones. In the same manner, the Ethernet switches are not located in the outer zones so that the communication network cannot be compromised by an attack.

(1) Figure 6-2 shows the switch interconnections and the self-healing ring. Any single switch failure would not compromise the network but would result in the isolation of only the zone to which that switch is assigned.

(2) The Zone 5 PLC monitors the "heartbeat" (signal) of each of the zone PLCs. Thus, in the event of a CBR attack or an explosion that destroys the Zone 1 PLC, the Zone 5 PLC would know within seconds and would react by isolating Zone 1.

c. In summary, there are six primary ways to initiate isolation of a peripheral zone from Zone 5, the command center:

(1) CBR detection by a zone PLC

(2) Fire or security alarm transmitted to a zone PLC

(3) Loss of communications signal from the zone PLC

(4) Failure of the Ethernet switch to the assigned zone

(5) A hardwired isolation pushbutton for each zone located in Zone 5

(6) A "soft" isolation pushbutton for each zone at the Zone 5 HMI.

6-7. Integration of functions

The example C4ISR facility has services for fire, security, electrical, and HVAC systems. The following describes the interface for each system.

a. The combined fire and security system has a local control panel in each of the peripheral zones, much like the PLC control system. Each panel should send two signals to the zone PLC: an alarm and a panel-in-operation signal. These signals are then sent to the SCADA system in the command center. Paragraph 7-4, Interface to SCADA System, provides further details of this interface.

b. Figure 6-1 shows the electrical system’s interface, which is detailed in paragraph 6-5, Reliability. Each zone PLC controls the electrical system equipment wired to a remote I/O rack.

c. Figure 6-1 shows the HVAC system's interface, which is detailed in paragraph 6-5, Reliability. Each zone PLC controls the HVAC system equipment connected to the PLC in that zone.